

BRACEWELL
& GIULIANI

Texas
New York
Washington, DC
Connecticut
Seattle
Dubai
London

Jonathan N. Halpern
Partner

212.508.6153 Office
212.938.3853 Fax

Jonathan.Halpern@bglp.com

Bracewell & Giuliani LLP
1251 Avenue of the Americas
49th Floor
New York, New York
10020-1104

November 7, 2013

By ECF AND HAND DELIVERY

The Honorable Paul G. Gardephe
United States District Judge
United States Courthouse
Southern District of New York
40 Foley Square
New York, New York 10007

Re: *United States v. Martoma*, 12 Cr. 973 (PGG)

Dear Judge Gardephe:

We respectfully submit this letter to the Court on behalf of Sidney Gilman, M.D., third-party intervenor, in response to Defendant Mathew Martoma's October 30, 2013 letter to the Court [Dkt. No. 90] ("Martoma Letter"), and in further support of Dr. Gilman's Motion for a Protective Order [Dkt. No. 46] and opposition to defendant Martoma's motion to compel.

The privacy and use policies that the University of Michigan ("University" or "UM") produced on October 24, 2013, pursuant to the Court's September 24, 2013 Order [Dkt. No. 75] ("Order"), highlight the premium that the University has placed on honoring the privacy of its faculty and other employees in their use of the University's computer system and electronic devices, especially for personal email use. Nonetheless, Mr. Martoma claims that the University of Michigan's policies and notices "confirm[]" that Dr. Gilman's communications on the University's Electronic Devices were not privileged because Dr. Gilman "could not have had a reasonable expectation of privacy with respect to such documents." Martoma Letter at 1. Mr. Martoma's characterization is inconsistent with the University's express policy statements, especially when viewed as a whole; undermined by the University's deferential action toward Dr. Gilman's assertions of privilege and requests for pre-production review; and unsupported by the law.

Far from banning personal use, the University has proclaimed that it "respects the privacy of its employees," *see* Ex. X, Morgenstern Decl. at UM-MM-000645 (The University of Michigan Faculty Handbook), and that it **"has fostered an environment which encourages the use of electronic email ... for both official and personal use."** **"It is the policy of the U-M that 'electronic mail is considered private to the fullest extent permitted by law.'" Ex. N, Morgenstern Decl. at UM-UM-000283, 291 (Standard Practice**



The Honorable Paul G. Gardephe

November 7, 2013

Page 2

Guide, Identification, Maintenance, and Preservation of Electronic Records, dated May 20, 1997) (emphasis added). It would be difficult to devise an employer policy that creates a work environment more conducive to an employee's having a reasonable expectation of privacy in using his employer's computer system for personal email -- especially confidential communications with one's lawyers and spouse.

Indeed, as discussed below, the policies, notices, and attestations produced by the University strongly support Dr. Gilman's reasonableness in his expectation of privacy and, accordingly, in his assertion of privilege over the personal documents and communications sent through and stored on the Electronic Devices. The complete record concerning the University's treatment of an employee's personal records stored on Electronic Devices makes clear that at no time during Dr. Gilman's tenure with the University¹ did the University: ban personal use of the Electronic Devices; warn that those devices were subject to routine or arbitrary monitoring; or notify employees that they had no expectation of privacy in the use of those devices. To the contrary, the clear message that the University uniformly conveyed to its employees was one of deference to employee autonomy in the electronic devices it issued to them and respect for their privacy, including in their personal and professional use.

This message of deference was specifically conveyed to Dr. Gilman by the University's own actions in agreeing to Dr. Gilman's privilege review requests -- especially when the University was required to produce Gilman-related emails and other electronic records under subpoena from the SEC or the government. The manner by which the University carried out its policies further demonstrates in practical terms its adherence to the University's commitment to upholding employee privacy and treating electronic mail and personal documents as private. *See* Declaration of Robert Frenchman, Esq. (attached).² In light of its policies, the manner that the University executed those policies as to Dr. Gilman and the applicable law, Dr. Gilman acted reasonably in fully expecting that his communications with his counsel and his wife would be private, confidential and privileged and that they would be treated accordingly.

¹ To clarify the term of his chairmanship and tenure at the University, Dr. Gilman was chairman of the Department of Neurology in the University's School of Medicine from 1977 until 2004, and he continued as a professor in the Department until his retirement in November 2012.

² The Frenchman Declaration sets forth a chronology and the context of events relating to Dr. Gilman's assertion of privilege, including assertions of privilege involving the University and the government.



The Honorable Paul G. Gardephe
November 7, 2013
Page 3

The University of Michigan's Production

Pursuant to this Court's Order, the University's production comprises employee handbooks, by-laws, standard practice guide provisions, and certain codes of conduct and attestations. *See* Declaration of Kara Morgenstern [Dkt. No. 84] ("Morgenstern Decl."). These documents reaffirm, first and foremost, that according to the dictates of its Electronic Policy the University of Michigan "respects the privacy of its employees and seeks to foster a climate free from arbitrary or capricious monitoring of its employees and the records they create, use or control." *See* Ex. O-3, Morgenstern Decl. at UM-MM -000325 (U-M Standard Practice Guide, Privacy and the Need to Monitor and Access Records); Ex. X, Morgenstern Decl. at UM-MM-000645 (The University of Michigan Faculty Handbook, Electronic Privacy (Winter 2008)).

Throughout Dr. Gilman's employment, the University's Faculty Handbook and other policies stressed the deference to employee privacy and the University's assurances that the highly-regarded privacy would be protected to the extent reasonably possible. For example:

- "The University of Michigan respects the privacy of its employees." *See* Ex. X, Morgenstern Decl. at UM-MM-000560 (Faculty Handbook, General Principles, Fall 2005).
- "University has fostered an environment which encourages the use of electronic mail, conference, and other communication systems **for both official and personal use. . . .** " **"It is the policy of the U-M that 'electronic mail is considered private to the fullest extent permitted by law.'"** Ex. N., Morgenstern Decl., at UM-MM-000283, 291 (Standard Practice Guide, Identification, Maintenance, and Preservation of Electronic Records, dated May 20, 1997) (emphasis added).
- "The intent of the policy is to protect personal communications of members of this [UM] community," except for communications within the definitions of "record," which do not include "[c]ommunication of personal or unofficial content;" in addition, private electronic mail was not required to be preserved in case a FOIA request is received in the future). *Id.* at 291-92 (emphasis added).

These policies and others produced by the University are readily distinguishable from the policies that this Court and other courts have held are incompatible with an employee's having a reasonable expectation of privacy in the personal use of his employer's computer and email systems. For example, in *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000), the court held that there was no reasonable expectation of privacy in the use of an



The Honorable Paul G. Gardephe

November 7, 2013

Page 4

office computer where the employer had a policy of auditing employees' use of the Internet). Similarly, in *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002), the court held that there was no reasonable expectation of privacy where the employer had announced that it could inspect the computer. See also *In re Reserve Fund Securities and Derivative Litig.*, 275 F.R.D. 154 (S.D.N.Y. 2011) (banning personal use); *Thygeson v. U.S. Bancorp*, 2004 WL 2066746 (D. Or. Sept. 15, 2004) (policy banned personal use and stated that email is the exclusive property of the company); *Kelleher v. City of Reading*, 2002 WL 106744 (E.D. Pa. 20002) (same); *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002) (employer reserved the right to inspect email at any time without prior notice).

In stark contrast, the University's policies tilt sharply in the opposite direction: to promote the protection of employee privacy in personal email use on the University computer system. This is hardly the kind of policy or position that is associated with clear notice to employees that their use of an employer's electronic system is not private.

Dr. Gilman's Expectation of Privacy In His Privileged Communications Was Reasonable

Dr. Gilman's expectation of privacy must be assessed in the context of the employment relation with the University, *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987), and in light of the reasonableness of his actions. *Convertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97, 110 (D.D.C. 2009). As articulated in *In re Asia Global Crossings*, and applied by this Court in *In re Reserve Fund*, whether an employee has a reasonable expectation of privacy in the use of an employer's electronic devices turns on the balancing of four factors: (1) whether the employer maintains a policy banning personal or objectionable use; (2) whether the employer monitors the use of the employee's computer or e-mail; (3) whether third parties have a right of access to the computer or e-mails; and (4) whether the employer notified the employee, or whether the employee was aware of the use and monitoring policies. *Asia Global Crossings*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005); *In re Reserve Fund*, 275 F.R.D. at 160. As set forth below, the produced policies, notices and attestations confirm that it was eminently reasonable for University employees, including Dr. Gilman, to expect that their confidential and personal communications would remain private.

The University's Policies Explicitly Permit Personal Use Of The Electronic Devices

First, the University's electronic use policies permit personal use of the Electronic Devices -- and the production indicates that historically the policies have done so. Beginning as early as 1993, the University made clear to its staff that "[a]t the University of Michigan, electronic mail and computer files are considered private to the fullest extent possible



The Honorable Paul G. Gardephe

November 7, 2013

Page 5

permitted by law.”³ In more recent years, including the period relevant to Dr. Gilman’s Motion (starting in the spring of 2012 with respect to the subject email communications with counsel) the University’s policy regarding “Privacy and the Need to Monitor and Access Records” (the “Privacy Policy”) expressly declares that the University “respects the privacy of its employees and seeks to foster a climate free from arbitrary and capricious monitoring of employees.”⁴ The Privacy Policy also states that:

[B]ecause the University permits some latitude for employees to use University resources to conduct University business off-campus and to conduct personal matters at their work sites, work-related records and employees’ personal records may be located in the same place.

Id. As these policies demonstrate, the University permitted its employees to use the Electronic Devices for personal matters, and, accordingly, Dr. Gilman’s use of the Electronic Devices to facilitate private communications with his counsel was entirely reasonable.⁵ See *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001) (employee had a reasonable expectation of privacy in the personal documents stored on his employer’s computer where the employer did not have a policy banning the storage of documents on company-issued computers); see *United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir.), *rev’d on other grounds*, 537 U.S. 802 (2002) (employee had reasonable expectation of privacy where his employer did not ban the storage of personal information on its computers); *Haynes v. Office of the Attorney General*, 298 F. Supp. 2d 1154, 1161-62 (D. Kan. 2003) (employee had reasonable expectation of privacy in personal files stored on employer’s computer where the employer allowed employees to use computers for personal communications); *United States v. Long*, 64 M.J. 57, 64 (C.A.A.F. 2006) (employee had reasonable expectation of privacy in her work computer where her employer did not restrict use of the computer to strictly business purposes); *Convertino*, 674 F. Supp. 2d 109-110 (employee had reasonable expectation of privacy in use of his employer’s email system where the employer did not ban personal use of the company email).

Mr. Martoma’s attempts to rewrite the law on privilege and privacy are similarly unavailing. Mr. Martoma contends that: (a) any limitation on personal use precluded an assertion of privilege; and (b) the absence of an absolute guarantee of privacy by the University defeated an assertion of privileged. See Martoma Letter (Dkt. No. 90) at 2-3.

³ See Morgenstern Decl., Ex. O-1, UM-MM-000308-309.

⁴ See Morgenstern Decl., Ex. O-3, UM-MM-000325

⁵ The University offers laptops to “employees who have a demonstrable business need for them and the [laptop is] used “[p]rimarily” (greater than 50 percent) for business reasons.” See Morgenstern Decl. at Ex. E-2, UM-MM-000126.



The Honorable Paul G. Gardephe
 November 7, 2013
 Page 6

First, there is no legal support for the proposition that any limitation on an employee's personal use of employer-issued electronic devices undermines the reasonableness of an employee's privacy expectation or defeats a claim of privilege. To the contrary, many courts have held that an employee's expectation of privacy was reasonable notwithstanding limitations on use that are substantially more restrictive than those in this case. *See Leventhal*, 266 F.3d at 73 (finding that employee had reasonable expectation of privacy in personal materials stored on his employer's computer notwithstanding the employer's anti-theft policy banning personal use of employer's computer system); *In re High-Tech Employee Antitrust Litig.*, 11-CV-2509-LHK-PSG, 2013 WL 772668 (N.D. Cal. Feb. 28, 2013) (reasonable expectation of privacy found where employer banned personal use "as a general rule"); *United States v. Nagle*, 09-CR-384, 2010 WL 3896200 (M.D. Pa. Sept. 30, 2010) (employee had a reasonable expectation of privacy where the employer did not prohibit personal use of the employer's computers, but merely excepted certain use as not private); *United States v. Hatfield*, 06-CR-0550 (JS), 2009 WL 3806300 (E.D.N.Y. Nov. 13, 2009) (favored finding of reasonable expectation of privacy where, under employer's policy, employees were expected to use their company equipment "solely for business purposes," even though the policy did not expressly prohibit personal use).

In addition, Martoma offers no legal support -- and none has been identified -- for the proposition that privacy and confidentiality must be guaranteed in order for a communication to qualify for the protection of privilege. To hold as such in today's electronic world in which electronic communications represent a controlling form of correspondence and have, in many instances, replaced written correspondence and in-person conversations would have dire and unwelcome consequences. For example, emailing through providers such as Gmail and Yahoo has been sanctioned by several state bars, including New York, as providing a sufficiently private and confidential method of communication between an attorney and client.⁶ A review of Gmail's privacy policy, however, makes clear that the email provider also does not guarantee the privacy of the communications; moreover, under its policy, Gmail may disclose personal information to individuals and entities for a wealth of reasons, well beyond the limited exceptions under the University's policy.⁷ It simply cannot be the case, nor is it so, as Mr. Martoma proposes, that Dr. Gilman's use of an electronic device or

⁶ *See, e.g.,* Raudebaugh, Kevin, *Trusting the Machines: New York State Bar Ethics Opinion Allows Attorneys to Use Gmail*, 6 Wash. J.L. Tech. & Arts 83 (2010).

⁷ For example, Gmail's privacy policy states that, among other reasons: "We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request; enforce applicable Terms of Service, including investigation of potential violations...." *Available at* <http://www.google.com/intl/en/policies/privacy/>.



The Honorable Paul G. Gardephe
November 7, 2013
Page 7

email system absent an absolute guarantee of privacy defeats a claim of confidentiality. The standard is a reasonable expectation of privacy, not an absolute expectation of privacy.

The University's Right To Access And Monitor The Electronic Devices Was Limited

The University's production confirms that the University does not routinely access or monitor the content of an employee's personal records.⁸ Apart from external legal requests, the University authorizes such limited contact only in two narrow situations, one of which is to obtain only embedded business, not personal, records; and the second, "[w]hen there is reasonable cause to believe that the employee has engaged in misconduct and may have used University resources improperly" (emphasis added). *See* Ex. O, Morgenstern Decl. at UM-UM-000326 (Privacy and Need to Monitor and Access Records dated September 7, 2004). Neither exception applies to the subject emails involving Dr. Gilman's communications with his lawyers or wife. This limited reservation of right to access and monitor personal records is consistent with UM's stated policy to protect the privacy interests of its employees. The University has sought to foster a climate "free from arbitrary or capricious monitoring" and has narrowly circumscribed its own monitoring and access rights. In fact, even where an intrusion is permitted under one exception, the University states that it will access records "only to the extent necessary" and only to obtain business records. *Id.*

The University's deference to employee autonomy and imposition of limitations on its own ability to monitor its employees' personal use of the Electronic Devices makes Dr. Gilman's expectation of privacy entirely reasonable. *See Leventhal*, 266 F.3d at 73 ("infrequent and selective search[es] for maintenance purposes" did not defeat employee's reasonable expectation of privacy in the storage of personal materials on his employer's computer); *In re High-Tech*, 2013 WL 772668 at *7 (reservation of right to access and monitor system did not destroy a reasonable expectation of privacy because the company did not actually monitor or access emails).

Even if there were a basis for the University to monitor or access certain of Dr. Gilman's personal records, as Mr. Martoma contends, none of the exceptions for intrusion identified by the policy justifies accessing Dr. Gilman's attorney-client privileged or protected materials, which were created long after any alleged wrongdoing on Dr. Gilman's part ended. Moreover, the University's policy regarding the investigation of allegations involving misconduct makes clear that, before any investigative action took place, the University would notify the employee. *See* Ex. B-4, Morgenstern Decl. at UM-MM 000074 – UM-MM 000077 (Procedures for Investigating Allegations of Misconduct in the Pursuit of Scholarship and Research).

⁸ *See* Morgenstern Decl. at pp., Ex. O-3, UM-MM-000325-000326.



The Honorable Paul G. Gardephe

November 7, 2013

Page 8

In addition, there has been no evidence that the University has monitored or reviewed Dr. Gilman's records that were retained on any Electronic Devices, including any communications that he had with his counsel. In fact, to the contrary, the University has honored Dr. Gilman's assertion of privilege and further acceded to his counsel's requests for pre-production privilege reviews. As the search protocol outlined in the July 3, 2013 Letter to the Court [Dkt. No. 42] explains, the University is deferring to the Court the issue of producing documents over which Dr. Gilman asserts privilege. *See* September 4, 2013 Letter to the Court and Frenchman Declaration.⁹

Dr. Gilman And The University Took Steps To Limit Third-Party Access And Disclosure

Mr. Martoma's assertion that the University's policies expressly permit third-party access to employee's personal records is similarly flawed. This factor focuses on the precautions the employee took to safeguard the device from third-party access, or whether obstacles hindered the employer from accessing privileged communications "despite having a policy or practice otherwise allowing the employer to do so." *See United States v. Finazzo*, No. 10-CR-475 (RMM), 2013 WL 619572 at * 10 (E.D.N.Y. Feb. 19, 2013). Here, the care and protection of the Electronic Devices demonstrates Dr. Gilman's expectation of privacy: his laptop and other Electronic Devices were provided by the University for his sole use; the Electronic Devices were password protected by a user-designated password and were either in his possession or stored in his private, locked office; and the laptop was encrypted by the University so that any unauthorized user could not access or review any data.

With respect to the University's FOIA obligations and the disclaimer that it may, under federal and state laws, be required to disclose certain records stored on the Electronic Devices, this disclosure is consistent with the obligations imposed on many electronic communication providers by federal and state laws and regulations. At most, the University's policies indicate that the University may need to review the contents of records, including personal records, in limited circumstances, to confirm the basis for exclusion of the

⁹ In his brief, Martoma states, without citation, that the "University subsequently acted . . . and reviewed Dr. Gilman's Electronic Media." Martoma Letter at 5. However, *see* Letter of Anthony S. Barkow, Esq., counsel for UM, dated July 22, 2013, at 1-2: the "University ran search terms against Dr. Gilman's Electronic Devices, without distinguishing between personal and professional files in response to law enforcement and/or regulatory requests." Running searches to identify documents is not the same as reviewing email content. And, as set forth in the Frenchman Declaration, the University permitted Dr. Gilman an opportunity to first screen for privileged documents captured by the searches. (Frenchman Decl. at ¶¶4-5).



The Honorable Paul G. Gardephe

November 7, 2013

Page 9

records from FOIA compliance.¹⁰ The University's stated effort to limit intrusions to those necessary for its independent compliance with federal and state laws is consistent with its stated policy against the arbitrary and capricious monitoring of Electronic Devices.¹¹

The University's Notices And Dr. Gilman's Acknowledgement Regarding The Policies Support Dr. Gilman's Reasonable Expectation Of Privacy

Fourth, Mr. Martoma has not produced, nor has the University provided, any support for Mr. Martoma's contention that Dr. Gilman was aware of the existence of any policy limiting his personal use of the Electronic Devices and impairing his expectation of privacy in the use of those devices. As previously stated, Dr. Gilman has not disputed the existence of policies governing his use of the Electronic Devices; however, he does not have a specific recollection of being made aware of such policies. See Dkt. No. 48, Gilman Decl. at ¶ 3. Indeed, the Code of Conduct Attestations provided by the University does not suggest otherwise. As late as 2009, the attestations with Dr. Gilman's signature (and attestations apparently electronically acknowledged in the years 2010, 2011 and 2012) concern employee compliance with the policies and procedures that apply to his work at the UM Health System.¹² Specifically, the attestation includes the statement: "I agree to comply with all of the policies and procedures that related to my work at UMHS, including the Code of Conduct. I agree that if I do not know whether an action is permitted, I will ask my supervisor or review the relevant policies." See Morgenstern Decl., Ex. BB-5, UM-MM-001519-001520.

The Code of Conduct Attestation does not identify all of the policies that related to Dr. Gilman's work, and does not specifically address the use of Electronic Devices or any privacy issues related to such use.¹³ Nonetheless, even assuming that the attestation and related Code of Conduct sufficiently placed Dr. Gilman on notice of the University's policies concerning Electronic Devices, those policies, as set forth above, make clear that Dr. Gilman is: permitted to use the devices for personal use; his personal records would be free from intrusion or monitoring; and third-party access would be extremely limited and subject only to compliance with federal or state laws (much the same as the terms of any email service

¹⁰ See Morgenstern Decl., Ex. KK, UM-MM-002360.

¹¹ See Morgenstern Decl., Ex. O-3, UM-MM-000325.

¹² See Morgenstern Decl. at Ex. BB, UM-MM-001519-001520.

¹³ It appears from the University's production that the University did not require Dr. Gilman to sign or acknowledge its privacy and use policies as related to University-supplied electronic devices. Nor did it warn him via a login screen, click-through mechanism or otherwise that his use of the University's electronic devices and systems was not private.



The Honorable Paul G. Gardephe
November 7, 2013
Page 10

provider). Thus, if anything, the policies would help reassure Dr. Gilman that his expectation of privacy with respect to his personal emails was entirely reasonable.

The University Has Complied With And Respected Dr. Gilman's Assertion Of Privilege

In addition to the four *In re Asia Global Factors*, in this case, the Court should consider the employment environment and the University's course of dealing with Dr. Gilman. Here, the employment environment is an academic setting in which employees, including medical professors with active research and patient practices, are expressly permitted to use the Electronic Devices to carry on personal activities. These include communicating with medical patients and legal counsel, without the fear of third-party monitoring or access. Moreover, under these particular circumstances, it is fundamentally unfair to declare, *retroactively*, that Dr. Gilman's personal, confidential and privileged communications should not be protected. This is especially so when the University has honored his privilege requests and apparently refrained from monitoring his communication with counsel. *See United States v. Hatfield*, No. 06-CR-0550, 2009 WL 3806300 at * 10 (E.D.N.Y. Nov. 13, 2009) (fundamentally unfair to find a waiver of privilege where employer recognized employee's privilege, permitted employee to conduct a privilege review of the materials stored on the employer's hard drive and refused to produce any material designated by the employee as privileged); *see also Curto v. Medical World Comm., Inc.*, No. 03-cv-6327, 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (holding that employer's failure to exercise its rights to monitor "lulled" the employee into a false sense of security in her personal use of employer-owned computer devices).

As set forth in detail in the Frenchman Declaration, Dr. Gilman's counsel repeatedly communicated with the University, asserted privilege on his behalf and requested opportunities to review subpoenaed files for privilege or protection. *See Frenchman Decl.* at ¶¶ 4-5. At no time since Dr. Gilman surrendered the Electronic Devices to the University did it object to his assertion of privilege. Nor did the University assert that there was a waiver or that Dr. Gilman had no reasonable expectation of privacy in light of the University's policies -- or for any other reason. The University honored Dr. Gilman's request to screen the Electronic Devices for privilege and work product protection. Dr. Gilman's counsel conducted a privilege review and provided the government with a privilege log. *See Frenchman Decl.* and September 4, 2013 Letter to the Court. Indeed, in light of the circumstances on the whole, the University's conduct has underscored the intent, spirit and letter of its policies and affirmed Dr. Gilman's reasonable expectation of privacy.

For the foregoing reasons and those in Dr. Gilman's previous submissions and arguments to the Court, it is respectfully submitted that Dr. Gilman's motion for a protective

BRACEWELL
& GIULIANI

The Honorable Paul G. Gardephe
November 7, 2013
Page 11

order be granted and that defendant Martoma's motion to compel be denied.

Respectfully submitted,

Bracewell & Giuliani LLP



Jonathan N. Halpern

cc: Roberto Braceras, Esq. (counsel for Defendant Mathew Martoma)
Richard Strassberg, Esq. (counsel for Defendant Mathew Martoma)
(by email)
AUSA Arlo Devlin-Brown
(by email)